COMMONWEALTH of VIRGINIA

Department of Medical Assistance Services

PATRICK W. FINNERTY
DIRECTOR

SUITE 1300
600 EAST BROAD ST
RICHMOND, VA 23219
804/786-7933
804/225-4512 (FAX)
800/343-0634 (TDD)

HIPAA BUSINESS ASSOCIATE CHAIN OF TRUST ATTACHMENT

THIS ATTACHMENT supplements and is made a part of the Business Associate Agreement (herein referred to as "Agreement") by and between the Department of Medical Assistance Services (herein referred to as "Covered Entity") and [name Business Associate] (herein referred to as "Business Associate").

BACKGROUND STATEMENTS

A. Covered Entity and Business Associate are parties to an agreement pursuant to which Business Associate provides certain services to Covered Entity and, in connection with those services, Covered Entity discloses to Business Associate certain information ("Protected Health Information" as further defined below) that is subject to protection under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Public Law 104-191; and

B. Business Associate, as a recipient of Protected Health Information (PHI) from Covered Entity, is a "Business Associate" as that term is defined in HIPAA and regulations promulgated by the U.S. Department of Health and Human Services (DHHS) to implement certain provisions of HIPAA (herein "HIPAA Regulations"); and

C. Pursuant to the HIPAA Regulations, all Business Associates of entities such as Covered Entity must, as a condition of doing business with Covered Entity, agree in writing to certain mandatory provisions regarding, among other things, the use and disclosure of PHI; and

D. The purpose of this Attachment is to satisfy the requirements of the HIPAA Regulations, including, but not limited to, 45 CFR § 164.506(e), as the same may be amended from time to time.

IN CONSIDERATION OF THE FOREGOING, and of the desire of each party to continue providing or receiving services under the Agreement, the parties agree as follows:

1. **Definitions.**

Unless otherwise provided in this Attachment, capitalized terms have the same meaning as set forth in the HIPAA Regulations, 45 CFR parts 142 and 160-164. As used in this contract, the terms below will have the following meanings:

a. Value-Added Network (VAN): A third party entity (e.g. vendor) that provides hardware and/or software communication services, which meet the security standards of telecommunication.

b. Encryption: A security measure process involving the conversion of data into a format, which cannot be interpreted by outside parties.

2. **Scope-of-Use of PHI.** Business Associate may not:

   a. Use or otherwise disclose PHI (as defined in 45 CFR §164.504) it receives from Covered Entity for any purpose other than the purpose expressly stated in the Agreement;

   b. Notwithstanding any other provisions of the Agreement, use or disclose PHI in the manner that violates or would violate the HIPAA regulations if such activity were engaged in by Covered Entity.

3. **Safeguards for the Protection of PHI.**

   a. Business Associate shall implement and maintain, and by this Agreement warrants that it has implemented, such safeguards as are necessary to ensure that the PHI disclosed by Covered Entity to Business Associate is not used or disclosed by Business Associate except as is provided in the Agreement.

   b. As detailed in the Data Security Plan Attachment, the Business Associate Data Security Plan shall be attached hereto and incorporated herein by reference and outline the safeguards implemented and maintained by Business Associate to prevent unauthorized use or disclosure of PHI. Business Associate warrants and represents that the information in the Business Associate Data Security Plan is true, correct and accurate and that one or more persons knowledgeable about Business Associate's security systems and procedures has completed the Business Associate Data Security Plan on behalf of Business Associate. Business Associate acknowledges that Covered Entity is relying on the Business Associate Data Security Plan in selecting Business Associate as a Business Partner. Business Associate shall promptly notify Covered Entity of any material change to any aspect of its security safeguards. Notwithstanding any other provisions of this Agreement to the contrary, Covered Entity may terminate the Agreement without penalty if it determines, in its sole discretion, that any such changes or any diminution of Business Associate's reported security procedures render any or all of Business Associate's safeguards unsatisfactory to Covered Entity. Business Associate shall confirm in writing to Covered Entity, from time to time upon Covered Entity's request, the continued accuracy of the Business Associate Data Security Plan.

4. **Reporting of Unauthorized Use or Disclosure.** Business Associate shall promptly report to Covered Entity any use or disclosure of PHI of which Business Associate becomes aware that is not provided for or permitted in the Agreement. Business Associate shall permit Covered Entity to investigate any such report and to examine Business Associate's premises, records and practices.

5. **Use of Subcontractors**. To the extent that Business Associate uses one or more subcontractors or agents to provide services under the Agreement, and such subcontractors or agents receive or have access to the PHI, each such subcontractor or agent shall sign an agreement with Business Associate containing substantially the same provisions as this Attachment and further identifying Covered Entity as a third party beneficiary with rights of enforcement and indemnification from such subcontractors or agents in the event of any violations.

6. **Uses of Open Communication Channels; Encryption**

   a. Business Associate may not transmit PHI over the Internet or any other insecure or open communication channel unless such information is encrypted or otherwise safeguarded using procedures no less stringent than those described in 45 CFR § 142.308(d).

   b. If Business Associate stores or maintains PHI in encrypted form, Business Associate shall, promptly at Covered Entity's request, provide Covered Entity with the key or keys to unlock such information.

7. **Electronic Data Interchange (EDI)**

   a. **Means of Transmission**

      i. Each party will transmit documents directly or through a third party value added network. Either party may select, or modify a selection of, a VAN upon thirty (30) days written notice.

ii. Each party will be solely responsible for the costs of any VAN with which it contracts.
iii. Each party will be liable to the other for the acts or omissions of its VAN while transmitting, receiving, storing or handling documents.
iv. Each party is solely responsible for complying with the subscription terms and conditions of the VAN he or she selects, and for any and all financial liabilities resulting from that subscription agreement.

b. **Test Data Transmission**
Each party agrees to actively send and receive test data transmissions until routinely successful. Supplier agrees to receive redundant transmissions (e.g. faxed copy and electronic), if required by Covered Entity, for up to thirty (30) days after a successful EDI link is established.

c. **Garbled Transmissions**
If a party receives an unintelligible document, that party will promptly notify the sending party (if identifiable from the received document). If the sending party is identifiable from the document but the receiving party failed to give notice that the document is unintelligible, the records of the sending party will govern. If the sending party is not identifiable from the document, the records of the party receiving the unintelligible document will govern.

d. **Signatures**
Each authorized representative of a party will adopt a unique, verifiable electronic identification consisting of symbols or codes to be transmitted with each document. Use of the electronic identification will be deemed for all purposes to constitute a "signature" and will have the same effect as a signature on a written document. Each authorized representative of a party will maintain sole control of the use of his or her signature, and neither party will disclose the signatures of the other party to any unauthorized person.

e. **Enforceability and Admissibility**
i. Any document properly transmitted pursuant to this Agreement will be deemed for all purposes (1) to be a "writing" or "in writing," and (2) to constitute an "original" when printed from electronic records established and maintained in the ordinary course of business.
ii. Any document which is transmitted pursuant to the EDI terms of this Agreement will be as legally sufficient as a written, signed, paper document exchanged between the parties, notwithstanding any legal requirement that the document be in writing or signed. Documents introduced as evidence in any judicial, arbitration, mediation or administrative proceeding will be admissible to the same extent as business records maintained in written form.

8. **Authorized Alteration of PHI.**

a. Business Associate acknowledges that the HIPAA regulations require Covered Entity to provide access to PHI to the subject of that information, if and when Business Associate makes any material alteration to such information. For purposes of this section, “Material Alteration” means any addition, deletion or change to the PHI of any subject other than the addition of indexing, coding or other administrative identifiers for the purpose of facilitating the identification or processing of such information.

b. Business Associate shall provide Covered Entity with notice of each material alteration to any PHI and shall cooperate promptly with Covered Entity in responding to any request made by any subject of such information to Covered Entity to inspect and/or copy such information.

c. Business Associate may not deny Covered Entity access to any such information if, in Covered Entity’s sole discretion, such information must be made available to the subject seeking access to it.

d. Business Associate shall promptly incorporate all amendments or corrections to PHI when notified by Covered Entity that such information is inaccurate or incomplete.

9. **Audits**, **Inspection and Enforcement.**

a. With reasonable notice, Covered Entity may inspect the facilities, systems, books and records of Business Associate to monitor compliance with this Attachment. Business Associate shall promptly remedy any violation of any term of this Attachment and shall certify the same to Covered Entity in writing. The fact the Covered Entity inspects, or fails to inspect, or has the right to inspect, Business Associate's facilities, systems and procedures does not relieve Business Associate of its responsibility to comply with this Attachment, nor does Covered Entity's failure to detect, or to detect but fail to call Business Associate's attention to or require Remediation of any unsatisfactory practice constitute acceptance of such practice or waiving of Covered Entity's enforcement rights.

b. Business Associate further agrees to make its internal practices, books and records relating to the use and disclosure of PHI available to the Department of Health and Human Services (DHHS) or its agents for the purposes of enforcing the provisions of this Attachment and the HIPAA regulations.

c. Covered Entity may terminate the Agreement without penalty if Business Associate repeatedly violates this Attachment or any provision hereof, irrespective of whether, or how promptly, Business Associate may remedy such violation after being notified of the same. In case of any such termination, Covered Entity shall not be liable for the payment of any services performed by Business Associate after the effective date of the termination, and Covered Entity shall be liable to Business Associate in accordance with the Agreement for services provided prior to the effective date of termination.

d. Business Associate acknowledges and agrees that any individual who is the subject of PHI disclosed by Covered Entity to Business Associate is a third party beneficiary of this Attachment and may, to the extent otherwise permitted by law, enforce directly against Business Associate any rights such individual may have under this Attachment, the Agreement, or any other law, relating to or arising out of Business Associate's violation of any provision of this Attachment.

10. **Effect of Termination.** Upon the termination of the Agreement for any reason, Business Associate will return to Covered Entity or, at Covered Entity's direction, destroy, all PHI received from Covered Entity that Business Associate maintains in any form, recorded on any medium, or stored in any storage system within thirty (30) days of termination or expiration of this Agreement. A senior officer of Business Associate shall certify in writing to Covered Entity, within thirty (30) days after the termination or other expiration of the Agreement, that all PHI has been returned or disposed of as provided above and that Business Associate no longer retains any such PHI in any form. Business Associate shall remain bound by the provisions of this Attachment, even after termination of the Agreement, until such time as all PHI has been returned or otherwise destroyed as provided in this section.

11. **Indemnification**. Business Associate shall indemnify and hold Covered Entity harmless from and against all claims, liabilities, judgments, fines, assessments, penalties, awards, or other expenses, of any kind or nature whatsoever, including, without limitation, attorney's fees, expert witness fees, and costs of investigation, litigation or dispute resolution, relating to or arising out of any breach or alleged breach of this Attachment by Business Associate.

12. Disclaimer. COVERED ENTITY MAKES NO WARRANTY OR REPRESENTATION THAT COMPLIANCE BY BUSINESS ASSOCIATE WITH THIS ATTACHMENT OR THE HIPAA REGULATIONS WILL BE ADEQUATE OR SATISFACTORY FOR BUSINESS ASSOCIATE'S OWN PURPOSES OR THAT ANY INFORMATION IN BUSINESS ASSOCIATE'S POSSESSION OR CONTROL, OR TRANSMITTED OR RECEIVED BY BUSINESS ASSOCIATE, IS OR WILL BE SECURE FROM UNAUTHORIZED USE OR DISCLOSURE, NOR SHALL COVERED ENTITY BE LIABLE TO BUSINESS ASSOCIATE FOR ANY CLAIM, LOSS OR DAMAGE RELATED TO THE UNAUTHORIZED USE OR DISCLOSURE OF ANY INFORMATION RECEIVED BY BUSINESS ASSOCIATE FROM COVERED ENTITY OR FROM ANY OTHER SOURCE. BUSINESS ASSOCIATE IS SOLELY RESPONSIBLE FOR ALL DECISIONS MADE BY BUSINESS ASSOCIATE REGARDING THE SAFEGUARDING OF PHI.

13. **Certification.** Subject to compliance with Business Associate's security requirements, Covered Entity, or its authorized agents or contractors, may at Covered Entity's cost examine Business Associate's facilities,

systems, procedures and records as may be required by such agents or contractors to certify to Covered Entity that Business Associate's security safeguards comply (or do not comply, as the case may be) with HIPAA, the HIPAA regulations, or this Attachment.

14. **Effect on Agreement.** Except as specifically required to implement the purposes of this Attachment, or to the extent inconsistent with this Attachment, all other terms of the Agreement shall remain in force and effect.

15. **Construction.** This Attachment shall be construed as broadly as necessary to implement and comply with HIPAA and the HIPAA Regulations. The parties agree that any ambiguity in this Attachment shall be resolved in favor of a meaning that complies and is consistent with HIPAA and the HIPAA Regulations.